scsi: pm8001: Fix use-after-free in pm8001_queue_command()

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-23306
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:26 UTC
Updated	2026-04-02 15:16:30 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free in pm8001_queue_comm

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000320000 probability, percentile 0.091780000 (date 2026-04-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e29c47fe8946cc732b0e0d393b65b13c84bb69d0 ebbb852ffbc952b95ddb7e3872b67b3e74c6da47 git
CNA	Linux	Linux	affected e29c47fe8946cc732b0e0d393b65b13c84bb69d0 8b00427317ba7b7ec91252b034009f638d0f311b gi
CNA	Linux	Linux	affected e29c47fe8946cc732b0e0d393b65b13c84bb69d0 c5dc39f8ae055520fd778b7fb0423f11586f15c4 git
CNA	Linux	Linux	affected e29c47fe8946cc732b0e0d393b65b13c84bb69d0 824a7672e3540962d5c77d4c6666254d7aa6f0b3 g
CNA	Linux	Linux	affected e29c47fe8946cc732b0e0d393b65b13c84bb69d0 227ff4af00abc40b95123cc27ee8079069dcd8d7 git
CNA	Linux	Linux	affected e29c47fe8946cc732b0e0d393b65b13c84bb69d0 38353c26db28efd984f51d426eac2396d299cca7 git
CNA	Linux	Linux	affected 5.18
CNA	Linux	Linux	unaffected 5.18 semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc2 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/38353c26db28efd984f51d426eac2396d299cca7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/227ff4af00abc40b95123cc27ee8079069dcd8d7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/824a7672e3540962d5c77d4c6666254d7aa6f0b3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c5dc39f8ae055520fd778b7fb0423f11586f15c4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ebbb852ffbc952b95ddb7e3872b67b3e74c6da47	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8b00427317ba7b7ec91252b034009f638d0f311b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.